(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10133953 A**

(43) Date of publication of application: **22 . 05 . 98**

(51) Int. Cl **G06F 12/14**
**G06K 17/00**

(21) Application number: **08302554**

(22) Date of filing: **28 . 10 . 96**

(71) Applicant: **TOKIMEC INC**

(72) Inventor: **KYOMASU TAKAFUMI**
**TERUYAMA KATSUYUKI**
**ATSUMI YOSHIO**

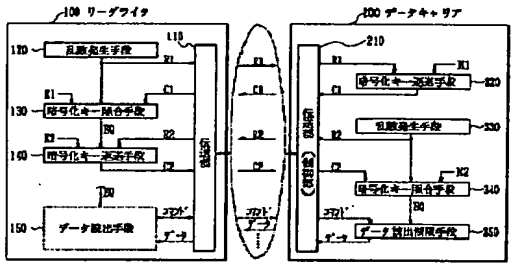
(54) **DATA SECRECY DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To protect memory data more securely against illegal use by interception by replacing the initiative side and answer side of a communication with each other by secrecy reset data is ciphered and multiplied.

SOLUTION: When a 1st random number is generated by a 1st random number generating means 120, sent from one communication device 10, and received by the other communication device 200, a 1st ciphering key sending-back means 320 ciphers 1st secrecy reset data with the 1st random number and sends it back to the communication device 100 from the communication device 200 and a 1st ciphering key matching means 130 matches it against a 1st ciphered secrecy reset data. According to this matching result, it is decided whether or not memory data can be sent and received. Prior to the transmission and reception of the memory data, the other communication device 200 takes the initiative to communicate with the communication device 100 as an answer side, and then 2nd secrecy data is confirmed.





(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－133953

(43)公開日　平成10年(1998)５月22日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｇ０６Ｆ　12/14 | ３２０ | Ｇ０６Ｆ　12/14 | ３２０Ｃ |
| | | | ３２０Ｂ |
| Ｇ０６Ｋ　17/00 | | Ｇ０６Ｋ　17/00 | Ｆ |
| | | | Ｓ |

審査請求　未請求　請求項の数３　ＦＤ　（全　９　頁）

(21)出願番号　特願平8－302554

(22)出願日　平成８年(1996)10月28日

(71)出願人　000003388
株式会社トキメック
東京都大田区南蒲田２丁目16番46号

(72)発明者　京増　貴文
東京都大田区南蒲田２丁目16番46号　株式会社トキメック内

(72)発明者　照山　勝幸
東京都大田区南蒲田２丁目16番46号　株式会社トキメック内

(72)発明者　渥美　凱雄
東京都大田区南蒲田２丁目16番46号　株式会社トキメック内

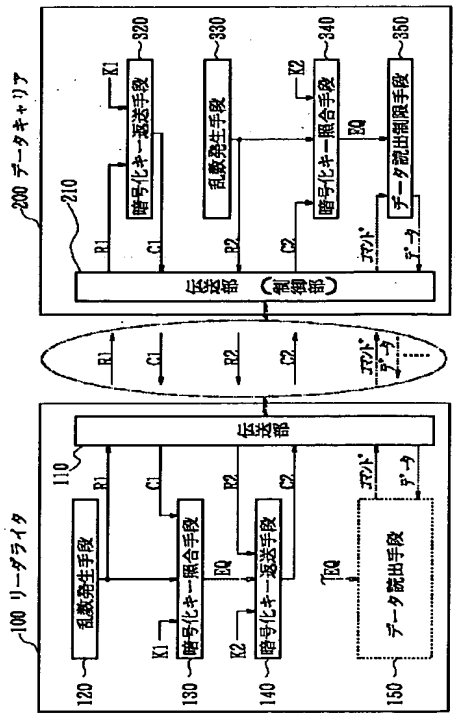
(74)代理人　弁理士　佐藤　香

(54)【発明の名称】　データ秘匿装置

(57)【要約】

【課題】通信を傍受しての不正使用から一層確実にメモリデータを保護する。

【解決手段】電磁誘導結合でのメモリデータの送受信に先だって秘匿解除データの送受信および照合を行うデータ秘匿装置において、乱数Ｒ１を発生する第１乱数発生手段１２０と、受信した乱数Ｒ１で秘匿解除データＫ１を暗号化し暗号化済み秘匿解除データＣ１を返送する第１暗号化キー返送手段３２０と、受信した暗号化済み秘匿解除データＣ１について照合を行う第１暗号化キー照合手段１３０と、乱数Ｒ２を発生する第２乱数発生手段３３０と、受信した乱数Ｒ２で秘匿解除データＫ２を暗号化し暗号化済み秘匿解除データＣ２を返送する第２暗号化キー返送手段１４０と、受信した暗号化済み秘匿解除データＣ２について照合を行う第２暗号化キー照合手段３４０とを備え、暗号化キー照合手段１４０，３４０の照合結果に基づいてメモリデータの送受信の可否を決する。



1

【特許請求の範囲】

【請求項１】電磁誘導結合に依り対をなしてメモリデータの送受信を行う一対のデータ通信装置に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータ秘匿装置において、前記一対のデータ通信装置のうちの一方の通信装置に設けられ第１の乱数を発生する第１乱数発生手段と、前記一対のデータ通信装置のうちの他方の通信装置に設けられ前記一方の通信装置から受信した前記第１の乱数を用いて第１の秘匿解除データを暗号化しこの暗号化済み第１の秘匿解除データを前記一方の通信装置へ返送する第１暗号化キー返送手段と、前記一方の通信装置に設けられ前記他方の通信装置から受信した暗号化済み第１の秘匿解除データについて照合を行う第１暗号化キー照合手段と、前記他方の通信装置に設けられ第２の乱数を発生するとともにこれを前記第１の秘匿解除データの返送の後に送信する第２乱数発生手段と、前記一方の通信装置に設けられ前記他方の通信装置から受信した前記第２の乱数を用いて第２の秘匿解除データを暗号化しこの暗号化済み第２の秘匿解除データを前記他方の通信装置へ返送する第２暗号化キー返送手段と、前記他方の通信装置に設けられ前記一方の通信装置から受信した暗号化済み第２の秘匿解除データについて照合を行う第２暗号化キー照合手段とを備え、前記第１暗号化キー照合手段および前記第２暗号化キー照合手段の照合結果に基づいて前記メモリデータの送受信の可否を決することを特徴とするデータ秘匿装置。

【請求項２】電磁誘導結合によってデータ記憶体とメモリデータの送受信を行うデータアクセス装置に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータアクセス装置のデータ秘匿装置において、第１の乱数を発生する乱数発生手段と、前記データ記憶体から受信した暗号化済み第１の秘匿解除データについて照合を行う暗号化キー照合手段と、前記データ記憶体から受信した第２の乱数を用いて第２の秘匿解除データを暗号化しこの暗号化済み第２の秘匿解除データを前記データ記憶体へ返送する暗号化キー返送手段とを備え、前記暗号化キー照合手段の照合結果に基づいて前記メモリデータの送受信の可否を決することを特徴とするデータアクセス装置のデータ秘匿装置。

【請求項３】電磁誘導結合によってデータアクセス装置とメモリデータの送受信を行うデータ記憶体に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータ記憶体のデータ秘匿装置において、前記データアクセス装置から受信した第１の乱数を用いて第１の秘匿解除データを暗号化しこの暗号化済み第１の秘匿解除データを前記データアクセス装置へ返送する暗号化キー返送手段と、第２の乱数を発生するとともにこれを前記第１の秘匿解除データの返送の後に送信する乱数発生手段と、前記データアクセス装置から受信した暗号化済み第２の秘匿解除データについて照合を行う暗号化キー照合手段とを備え、前記暗号化キー照合手段の照合結果に基づいて前記メモリデータの送受信の可否を決することを特徴とするデータ記憶体のデータ秘匿装置。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、データ秘匿装置に関し、詳しくは、交番電磁界を用いた電磁誘導結合方式で通信するデータ通信装置に好適なデータ秘匿装置に関する。かかるデータ通信装置は、ＩＣカードやデータキャリア等の（携帯形）データ記憶体と、これ又はこれらのうち通信可能なところまで近接したデータ記憶体に対し通信でアクセスして接触不要でデータの読み取り，書き込み，又は読み書きを行うリーダ等のデータアクセス装置とからなる。

【０００２】そして、その内部回路は要部がＩＣ化されていて解析・解読が設備・コスト面から困難なものとなっており、さらに、その通信方式では通信可能な地域的範囲が狭く且つ交信手順が非公開となっている。そのため、このデータ秘匿装置は、通信伝文を監視して得た情報に基づいてデータ記憶体のデータを書き換えようとする行為を主対象とすることで、一般の秘話装置よりも簡便な方式により、不正行為からデータ記憶体のデータを保護しようとするものである。

【０００３】

【従来の技術】携帯形データ記憶体のデータに電磁誘導結合方式の通信でアクセスするデータアクセス装置の適用例として、図４（ａ）にブロック図で示したデータキャリアシステムが挙げられる。このシステムは、屋外や構築物あるいは車両・船舶等に据えて設置されるリーダライタ１０（データアクセス装置）と、携帯に好適な小形サイズのデータキャリア２０（データ記憶体）とからなるものである。極めて小規模なシステムではこの一対だけでも済むが、通常は、単一又は複数のリーダライタ１０に対して多数のデータキャリア２０が用いられ、リーダライタ１０と通信可能な近距離にまで接近したデータキャリア２０とが所定データの送受に要する短時間だけ動的に対を確立するようになっている。

【０００４】リーダライタ１０は、商用電力ＡＣ１００Ｖの供給を受けて作動するものであり、マイクロプロセッサ１４を有して、そのプログラム処理によって電力送給波やコマンドあるいは書き込みデータなどの送出を制御するようになっている。さらに、マイクロプロセッサ１４の制御下で電力送給波等を交番電磁界としてデータキャリア２０へ向けて出射するために、送信データ等で所定周波数の搬送波を変調する変調回路や変調済み送信

信号をパワー増幅する送信アンプ等からなる伝送部１３と、送信信号を交番電磁界に変換するコイル１１とを備えたものとなっている。

【０００５】データキャリア２０は、動作電力の供給をリーダライタ２０から非接触で受けるために、交番電磁界による電力送給波等を受けるコイル２１と、これで受けた電力送給波を整流・蓄電等して電源電圧を生成する整流回路２２とを備えたものである。コイル２１はコマンド等の受信コイルでもあり、コイル１１からの交番電磁界によってコイル２１に誘起した信号は、制御部２３によって受理される。制御回路２３は、コイル２１の誘起信号を増幅する受信アンプや搬送波を除去する復調回路等からなる伝送部も兼ねたものとなっている。制御回路２３は、受信したコマンドの内容に応じてチップセレクトＣＳ，シフトクロックＳＫ，受信データＤＩ等の制御信号を生成し、これでメモリ２４にアクセスしてデータの書き込み等を行うようになっている。

【０００６】また、データキャリア２０の伝送部には、送信処理のために変調回路や送信アンプも具備されており、コマンドの処理結果や、メモリ２４からの読出データＤＯなどの送信信号は、制御回路２３の制御に従って、変調回路によって搬送波に混合され、送信アンプによってパワー増幅されてから、コイル２１を介して交番電磁界に変換・出射されるようになっている。

【０００７】さらに、リーダライタ１０の伝送部１３には、データキャリア２０の送信信号を受信するために、データキャリア２０からの交番電磁界によってコイル１１に誘起した誘起信号を増幅する受信アンプや、この信号から搬送波成分やノイズ成分を除去して復調する復調回路も具備されている。そして、マイクロプロセッサ１４のプログラム処理によって、復調信号からデータを抽出したり、コマンド処理結果を確認する等の処理を行うようになっている。

【０００８】かかるデータキャリアシステムでは、データキャリア２０が電磁誘導結合による供給電力や小さな内蔵電池によって動作することから、データキャリア２０のコイル２１から出射される交番電磁界は微弱であり、通信可能な地域的範囲が狭い。そして、このようなデータキャリアシステムは、スキー場でのリフト搭乗券改札システムや乗合バス乗車券改札システムなどに応用される。この場合、各改札にリーダライタ１０が設置され、多数のデータキャリア２０はリストバンド状や切符状に形成されていて搭乗券・乗車券の代わりに各利用者によって所持される。さらに、各データキャリア２０のメモリ２４には、搭乗可能か否かの搭乗券情報や支払い済み料金の残額等がメモリデータとして保持されている。

【０００９】そして、搭乗等の際に利用者が自己のデータキャリア２０をリーダライタ１０のコイル２１に近づけてこれら一対のリーダライタ１０及びデータキャリア２０が交信可能な状態になると、メモリデータの送受信が行われる。すなわち、リーダライタ１０がデータキャリア２０へ読出コマンド（リードコマンド）を送出し、これを受けてデータキャリア２０がメモリ２４から保持データを読み出してこれをリーダライタ１０へ返送する。さらに、リーダライタ１０はデータの内容をチェックし、データ更新の必要があると、リーダライタ１０がデータキャリア２０へ更新データと共に書込コマンドを送出し、これを受けてデータキャリア２０がメモリ２４の保持データを書き換えるのである。

【００１０】従来のデータ秘匿装置は、このようなメモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことでメモリデータの送受信の可否を決するためにデータキャリアシステムに対して付加・内蔵されるものであり、特開平４－１６９９９０号公報記載のものが挙げられる。これは、リーダライタ１０におけるマイクロプロセッサ１４について、リードコマンドと一緒に所定値の秘匿解除データも送信するようにプログラム処理が改められるとともに（図４（ｂ）参照）、データキャリア２０については、秘匿解除データ（キー）の照合および送受信可否の判定を行う秘匿回路３０と、秘匿回路３０の判定結果に従ってメモリデータの読み出しを制限するために読出データＤＯの信号ラインに介挿され読出データＤＯ以外の入力として秘匿回路３０の判定結果の信号を受けるＡＮＤゲート４１とが設けられたものである。

【００１１】秘匿回路３０は、受信データＤＩをシリアル入力としシフトクロックＳＫをタイミング信号とするシフトレジスタ３１を有してこれにリーダライタ１０からの受信秘匿解除データをロードする一方で、読出データＤＯをシリアル入力としシフトクロックＳＫをタイミング信号とするシフトレジスタ３２を有してこれにメモリ２４の所定アドレスから読み出した読出秘匿解除データ等をロードするとともに、シフトレジスタ３１，３２のパラレル出力を両入力としこれらがする一致しているか否かの一致出力ＥＱを生成出力する比較回路３３を有して両秘匿解除データの照合を行う。さらに、シフトクロックＳＫのカウンタ３４によるカウント値ＣＮＴを状態遷移の基準信号とする順序回路３５を有し、この順序回路３５で一致出力ＥＱを全ビットに亘って監視し、両秘匿解除データが完全に一致しているときだけ、データ読出の制限を解除する信号がＡＮＤゲート４１に送出されるようになっている。

【００１２】このように秘匿解除データをデータアクセス装置から送信しそれをデータ記憶体で照合することで比較的簡便に、秘匿解除データが知られない限り不正行為からデータ記憶体のデータが保護される。一般にデータキャリアシステムは内部回路がＩＣ化されることに加えて通信可能な地域的範囲が狭く且つ交信手順も公開されないので、第三者の秘匿解除データ取得は困難であ

る。

【００１３】

【発明が解決しようとする課題】しかしながら、このような従来のデータ秘匿装置では、秘匿解除データがそのまま通信伝文に含められている。このため、例え秘匿解除データ取得のための通信伝文傍受等が困難とは言っても、何らかの方策によって通信伝文が一旦傍受等された場合まで想定すると、秘匿解除データの特定・抽出に対する保護が万全とはいえない。また、通信手順も常時交互になされるので推定・把握しやすいといえる。そこで、通信傍受等により通信伝文を監視して得た情報に基づいてデータ記憶体のデータを書き換えようとする行為に対しても、一般の秘話装置よりも簡便な方式で、データ記憶体のデータを秘匿して保護することが課題となる。

【００１４】この発明は、このような課題を解決するためになされたものであり、通信を傍受しての不正使用から一層確実にメモリデータを保護するデータ秘匿装置を実現することを目的とする。

【００１５】

【課題を解決するための手段】このような課題を解決するためになされた本発明について、その構成および作用効果を以下に説明する。なお、図１の機能ブロック図の符号も併記する。

【００１６】この解決手段のデータ秘匿装置は（、出願当初の請求項１に記載の如く）、（互いのコイルやアンテナ等の間に確立された）電磁誘導結合に依り（一時的な又は恒常的な）対をなして（メモリからの読出データ及びメモリへの書込データの何れか一方または双方の）メモリデータの送受信を行う一対のデータ通信装置に具備され、前記メモリデータの送受信に先だって秘匿解除データの送受信および照合を行うことで前記メモリデータの送受信の可否を決するデータ秘匿装置において、前記一対のデータ通信装置のうちの一方の通信装置（１００）に設けられ、第１の乱数（Ｒ１）を発生する第１乱数発生手段（１２０）と、前記一対のデータ通信装置のうちの他方の通信装置（２００）に設けられ、前記一方の通信装置（１００）から受信した前記第１の乱数（Ｒ１）を用いて第１の秘匿解除データ（Ｋ１）を暗号化しこの暗号化済み第１の秘匿解除データ（Ｃ１）を前記一方の通信装置（１００）へ返送する第１暗号化キー返送手段（３２０）と、前記一方の通信装置（１００）に設けられ、前記他方の通信装置（２００）から受信した暗号化済み第１の秘匿解除データ（Ｃ１）について（自己の保持する第１の秘匿解除データ（Ｋ１）との）照合を行う第１暗号化キー照合手段（１３０）と、前記他方の通信装置（２００）に設けられ、第２の乱数（Ｒ２）を発生するとともに、これを前記第１の秘匿解除データ（Ｃ１）の返送の後に（直ちに又は所定時間経過してから）送信する第２乱数発生手段（３３０）と、前記一方の通信装置（１００）に設けられ、前記他方の通信装置（２００）から受信した前記第２の乱数（Ｒ２）を用いて第２の秘匿解除データ（Ｋ２）を暗号化しこの暗号化済み第２の秘匿解除データ（Ｃ２）を前記他方の通信装置（２００）へ返送する第２暗号化キー返送手段（１４０）と、前記他方の通信装置（２００）に設けられ、前記一方の通信装置（１００）から受信した暗号化済み第２の秘匿解除データ（Ｃ２）について（自己の保持する第２の秘匿解除データ（Ｋ２）との）照合を行う第２暗号化キー照合手段（３４０）とを備え、前記第１暗号化キー照合手段（１３０）および前記第２暗号化キー照合手段（３４０）の照合結果に基づいて前記メモリデータの送受信の可否を決する（１５０，３５０）ことを特徴とするものである。

【００１７】このようなデータ秘匿装置にあっては、電磁誘導結合に依って対をなす一対のデータ通信装置間でメモリデータの送受信を行うに際し、データ改竄等の不正使用からメモリデータを保護するために、メモリデータの送受信に先だって秘匿解除データの送受信および照合が行われてメモリデータの送受信の可否が決定されるのであるが、保護強化のために特に秘匿解除データの送受信および照合が以下の如く行われる。

【００１８】すなわち、第１乱数発生手段によって第１の乱数が生成され、これが一方の通信装置から送信されて他方の通信装置で受信されると、第１暗号化キー返送手段によって、第１の秘匿解除データがその第１の乱数で暗号化されて他方の通信装置から一方の通信装置へ返送され、さらに、第１暗号化キー照合手段によって、暗号化済み第１の秘匿解除データについて照合が行われる。そして、この照合結果に基づいてメモリデータの送受信の可否が決せられる。

【００１９】こうして、メモリデータの送受信に先だって一方の通信装置が主導し他方の通信装置が応答する交信が行われ、これに基づいて第１の秘匿解除データの確認が行われることから、第１の秘匿解除データを知らない者はメモリデータの送受信を始めることができないので、そのような者の不正使用からデータを秘匿し保護することができる。しかも、秘匿解除データが乱数で暗号化されて送受信の度に変化するので、送信伝文が傍受・監視されたとしても、秘匿解除データが特定・抽出されるおそれは、ほとんど無い。

【００２０】また、引き続き、第２乱数発生手段によって第２の乱数が生成され、これが他方の通信装置から送信されて一方の通信装置で受信されると、第２暗号化キー返送手段によって、第２の秘匿解除データがその第２の乱数で暗号化されて一方の通信装置から他方の通信装置へ返送され、さらに、第２暗号化キー照合手段によって、暗号化済み第２の秘匿解除データについて照合が行われる。そして、この照合結果に基づいても、メモリデータの送受信の可否が決せられる。

【００２１】こうして、メモリデータの送受信に先だって先ほどとは逆に他方の通信装置が主導し一方の通信装置が応答する交信が行われ、これに基づいて第２の秘匿解除データの確認が行われることから、第２の秘匿解除データを知らない者はメモリデータの送受信を始めることができないので、そのような者の不正使用からデータを秘匿し保護することができる。しかも、秘匿解除データが乱数で暗号化されて送受信の度に変化するので、送信伝文が傍受・監視されたとしても、秘匿解除データが特定・抽出されるおそれは、ほとんど無い。

【００２２】しかも、電磁誘導結合によるデータ通信装置の場合この電磁誘導結合を介して一方の通信装置から他方の通信装置へエネルギー供給がなされることが多い等のため一方の通信装置が主導し他方の通信装置が応答する手順でメモリデータの送受信が行われのが通例であるところ、逆に他方の通信装置が主導し一方の通信装置が応答する交信も組み合わせられている。このように主導する側が動的に入れ替わること及びそのタイミングを送信伝文の傍受・監視によって検知することは困難である。

【００２３】これにより、単に秘匿解除データを暗号化および複数化したことを超えて、より確実に、不正使用からメモリデータが保護される。したがって、この発明によれば、従来よりも確実に不正使用からメモリデータを保護することができる。

【００２４】

【発明の実施の形態】このような解決手段で達成された本発明のデータ秘匿装置について、これを実施するための形態を説明する。

【００２５】［第１の実施の形態］本発明の第１の実施形態は、上述した解決手段のデータ秘匿装置であって、前記一方の通信装置（１００）が（、出願当初の請求項２に記載の如く）、上記の第１乱数発生手段（１２０）と第１暗号化キー照合手段（１３０）と第２暗号化キー返送手段（１４０）と前記第１暗号化キー照合手段（１３０）の照合結果に基づいて前記メモリデータの送受信の可否を決するデータ読出手段（１５０）とを備えたデータアクセス装置（データ読取装置、データ書込装置、データ読書装置）であり、前記他方の通信装置（２００）が（、出願当初の請求項３に記載の如く）、上記の第１暗号化キー返送手段（３２０）と第２乱数発生手段（３３０）と第２暗号化キー照合手段（３４０）と前記第２暗号化キー照合手段（３４０）の照合結果に基づいて前記メモリデータの送受信の可否を決するデータ読出制限手段（３５０）とを備えたデータ記憶体である。これにより、データ記憶体の保持する（期日や金額等の）メモリデータを改竄すること等の不正使用が、ほぼ不可能となる。

【００２６】［第２の実施の形態］本発明の第２の実施形態は、上述した解決手段および実施形態のデータ秘匿装置が、他の複数装置とともに利用地域や利用日等の所定基準に従ってグループ分けされており、前記第１の秘匿解除データ及び前記第２の秘匿解除データの少なくとも一方は少なくとも一部が前記グループ分けに対応して設定されていることを特徴とする。これにより、異なるグループ間での不正流用を容易かつ確実に防止することができる。

【００２７】例えば本発明のデータ秘匿装置が組み込まれたリーダライタ１００（データ読取装置）及びデータキャリア２００（データ記憶体）を自動改札装置およびリフト搭乗券として複数のスキー場に導入したような場合、各スキー場ごとに異ならせてキーＫ１（第１の秘匿解除データ）の値を設定するとともに、利用日ごとに異ならせてキーＫ２（第２の秘匿解除データ）の値を設定するとよい。こうすることで、新たな回路等を何ら付加しなくても、他のスキーのリフト券や前日のリフト券などについての改札誤りを避けることが可能となる。

【００２８】

【実施例】本発明のデータ秘匿装置を適用した一実施例としてのデータキャリアシステムについて、その具体的な構成を、図面を引用して説明する。図１は、その機能ブロック図であり、図２は、データアクセス装置としてのリーダライタ１００の回路ブロック図およびフローチャートであり、図３は、データ記憶体としてのデータキャリア２００の回路ブロック図である。

【００２９】リーダライタ１００は、マイクロプロセッサ１４のプログラム処理が第１乱数発生手段１２０と第１暗号化キー照合手段１３０と第２暗号化キー返送手段１４０とを具現化するように変更されている点で、従来例におけるリーダライタ１０と相違する。データキャリア２００は、秘匿回路３００が第１暗号化キー返送手段３２０と第２乱数発生手段３３０と第２暗号化キー照合手段３４０とを具現化するように秘匿回路３０から拡張されている点で、従来例におけるデータキャリア２０と相違する。なお、図１では、コイル１１と伝送部１３とを纏めて伝送部１１０とし、コイル２１と制御回路２３０等とを纏めて伝送部２１０として示した。以下、重複する再度の説明は割愛し、これらの相違点を説明する。

【００３０】リーダライタ１００のマイクロプロセッサ１４は、データキャリア２００と交信可能になると、先ず、乱数Ｒ１（第１の乱数）を発生するようにプログラムされている（図２のステップＳ１を参照）。乱数発生は、一般的な疑似乱数を発生させるものでよく、シフトと加算とを繰り返しその度に一部を抽出して乱数とすること等で具体化され、乱数Ｒ１の値は毎回変化する。これにより、リーダライタ１００は、第１の乱数Ｒ１を発生する第１乱数発生手段１２０を備えたものとなっている。さらに、マイクロプロセッサ１４は、この乱数Ｒ１を伝送部１３及びコイル１１経由で交番電磁界として送出するようにもプログラムされている（ステップＳ

２）。これにより、乱数Ｒ１がデータキャリア２００へ送信されるようになっている。

【００３１】リーダライタ１００のマイクロプロセッサ１４は、その後、データキャリア２００からの返信（Ｃ１）を待ってこれを受信する（ステップＳ３）。この返信（Ｃ１）はデータキャリア２００によってキーＫ１（第１の秘匿解除データ）が乱数Ｒ１で暗号化された暗号化キーＣ１（暗号化済み第１の秘匿解除データ）であることが期待されており、この暗号化キーＣ１に対して暗号化と逆の復号化処理が乱数Ｒ１を用いて施され、復号化した値Ｆ１を得る（ステップＳ４）。さらに、値Ｆ１がマイクロプロセッサ１４付属のメモリに記憶済みのキーＫ１と同一値か否かを判別する（ステップＳ５）。これにより、リーダライタ１００は、受信した暗号化キーＣ１について自己の保持するキーＫ１との照合を行う第１暗号化キー照合手段１３０を備えたものとなっている。

【００３２】そして、比較結果が不一致のときにはその時点でそのデータキャリア２００を対象とした通信を停止するが、比較結果が一致のときにはさらに以下の処理を続行する（ステップＳ５）。リーダライタ１００のマイクロプロセッサ１４は、引き続き、データキャリア２００から乱数Ｒ２（第２の乱数）が送信されて来るのを待ってこれを受信すると（ステップＳ６）、この乱数Ｒ２を用いてキーＫ２（第２の秘匿解除データ）に暗号化処理を施して暗号化キーＣ２（暗号化済み第２の秘匿解除データ）を生成する（ステップＳ７）。この暗号化処理は掛け算あるいは排他的論理和などで具現化され、暗号化キーＣ２は、データキャリア２００へ向けて送出され返送される（ステップＳ８）。これにより、リーダライタ１００は、受信した乱数Ｒ２を用いてキーＫ２を暗号化しこの暗号化キーＣ２をデータキャリア２００へ返送する第２暗号化キー返送手段１４０を備えたものとなっている。

【００３３】そして、これらの一連の処理を終えてから、さらにデータキャリア２００の準備が整うまでの所定時間が経過してから、本来のデータ読出等を開始するためにリードコマンドの送信を行う。しかも、上述したように暗号化キーＣ１とキーＫ１との比較結果が一致したときだけ、リードコマンドの送信を開始する。これにより、リーダライタ１００は、第１暗号化キー照合手段１３０の照合結果に基づいてメモリデータの送受信の可否を決するデータ読出手段１５０を備えたものとなっている。

【００３４】データキャリア２００の秘匿回路３００は、秘匿回路３０に設けられていたシフトレジスタ３１，３２と比較回路３３とカウンタ３４と順序回路３５とに加えて、受信データＤＩをシリアル入力としシフトクロックＳＫをタイミング信号とするシフトレジスタ３０１と、読出データＤＯをシリアル入力としシフトクロックＳＫをタイミング信号とするシフトレジスタ３０２と、両シフトレジスタ３０１，３０２に保持されたデータに掛け算等の処理を施して暗号化する暗号化回路３０３とが設けられている。そして、リーダライタ１００から乱数Ｒ１を受信すると、この乱数Ｒ１が受信データＤＩとしてシフトレジスタ３０１にロードされるとともにキーＫ１が読出データＤＯとしてシフトレジスタ３０２にロードされて、暗号化回路３０３によって暗号化キーＣ１が生成されるようになっている。また、制御回路２３０は、乱数Ｒ１の受信時にそのような制御を行うとともに暗号化キーＣ１をリーダライタ１００へ返送するように制御回路２３が改造されたものである。これにより、データキャリア２００は、受信した乱数Ｒ１を用いてキーＫ１を暗号化しこの暗号化キーＣ１をリーダライタ１００へ返送する第１暗号化キー返送手段３２０を備えたものとなっている。

【００３５】また、秘匿回路３００に、疑似乱数を算出することで発生ごとに値の変化する乱数Ｒ２を発生する乱数発生回路３０４が設けられるとともに、制御回路２３０に、暗号化キーＣ１の返送後これに続けて乱数Ｒ２をリーダライタ１００へ送信するような制御シーケンスが付加されている。これにより、データキャリア２００は、乱数Ｒ２を発生するとともにこれを暗号化キーＣ１の返送の後に送信する第２乱数発生手段３３０を備えたものとなっている。

【００３６】さらに、秘匿回路３００には、乱数Ｒ２を受けて保持するシフトレジスタ３０５と、シフトレジスタ３２と比較回路３３との間に介挿されシフトレジスタ３２のキーＫ２をシフトレジスタ３０５の乱数Ｒ２で暗号化（Ｆ２）してから比較回路３３へ送出する暗号化回路３０６とが設けられ、制御回路２３０は、乱数Ｒ２の送信後に暗号化キーＣ２を受信して初めて、これをシフトレジスタ３１にロードさせ、比較回路３３，カウンタ３４，順序回路３５を動作させるものである。これにより、データキャリア２００は、受信した暗号化キーＣ２について自己の保持するキーＫ２との照合を行う第２暗号化キー照合手段３４０を備えたものとなっている。なお、順序回路３５の出力を受けるＡＮＤゲート４１の存在により、第２暗号化キー照合手段３４０の照合結果に基づいてメモリデータの送受信の可否を決するデータ読出制限手段３５０も備えたものとなっている。

【００３７】このようなリーダライタ１００及びデータキャリア２００内に具現化されたデータ秘匿装置について、その使用態様及び動作を説明する。

【００３８】かかるデータキャリアシステムでは、利用者が自己のデータキャリア２００をリーダライタ１００のコイル２１に近づけてこれら一対のリーダライタ１００及びデータキャリア２００が交信可能な状態になると、先ず、リーダライタ１００が主導する秘匿解除データＫ１についての送受信および照合と、データキャリア

２００が主導する秘匿解除データＫ２についての送受信および照合とがおこなわる。

【００３９】秘匿解除データＫ１についての送受信および照合は、リーダライタ１００の乱数発生手段１２０による乱数Ｒ１の発生およびその送信によって開始され、この乱数Ｒ１を受けたデータキャリア２００の暗号化キー返送手段３２０による暗号化キーＣ１の返送で継続され、リーダライタ１００の暗号化キー照合手段１３０による暗号化キーＣ１とキーＫ１との照合によって終了する。こうして、リーダライタ１００からデータキャリア２００へ乱数Ｒ１の通信伝文が送られるとともにデータキャリア２００からリーダライタ１００へ暗号化キーＣ１の通信伝文が送り返される（図１における二点鎖線内を参照）。そして、乱数Ｒ１が毎回変化するので、暗号化キーＣ１も毎回変化し、キーＫ１は生の値が通信伝文に現れるということがない。

【００４０】秘匿解除データＫ２についての送受信および照合は、データキャリア２００の乱数発生手段３３０による乱数Ｒ２の発生およびその送信によって開始され、この乱数Ｒ２を受けたリーダライタ１００の暗号化キー返送手段１４０による暗号化キーＣ２の返送で継続され、データキャリア２００の暗号化キー照合手段３４０による暗号化キーＣ２とキーＫ２との照合によって終了する。こうして、データキャリア２００からもリーダライタ１００へ乱数Ｒ２の通信伝文が送られるとともにリーダライタ１００からデータキャリア２００へ暗号化キーＣ２の通信伝文が送り返される（図１の二点鎖線内参照）。そして、この場合も、乱数Ｒ２，暗号化キーＣ２が毎回変化するので、キーＫ２は生の値が通信伝文に現れるということがない。

【００４１】そして、リーダライタ１００においてキーＫ２の一致照合が成立し、さらにデータキャリア２００においてもキーＫ１の一致照合が成立した場合だけ、メモリデータの送受信が行われる。すなわち、リーダライタ１００がデータキャリア２００へリードコマンドを送出し、これを受けてデータキャリア２００がメモリ２４から保持データを読み出してこれをリーダライタ１００へ返送するなどの交信に基づく通常の処理が継続される（図１の二点鎖線内参照）。

【００４２】こうして、リーダライタ１００の主導する乱数Ｒ１及び暗号化キーＣ１の交信と、同じくリーダライタ１００の主導するコマンド及びデータの交信との間に、それらとは逆にデータキャリア２００の主導する乱数Ｒ２及び暗号化キーＣ２の交信が挿入されることで、メモリデータの送受信に先だつ秘匿解除データの送受信および照合が行われる。

【００４３】

【発明の効果】以上の説明から明らかなように、本発明のデータ秘匿装置にあっては、傍受した通信の解読を困難にするため秘匿解除データを暗号化および複数化するに際し、交信の主導側および応答側が入れ替わるようにしたことにより、一層確実に不正使用からメモリデータを保護することができたという有利な効果が有る。

【図面の簡単な説明】

【図１】　本発明のデータ秘匿装置について、機能ブロック図である。

【図２】　そのデータ読取装置についての回路等ブロック図である。

【図３】　そのデータ記憶体についての回路ブロック図である。

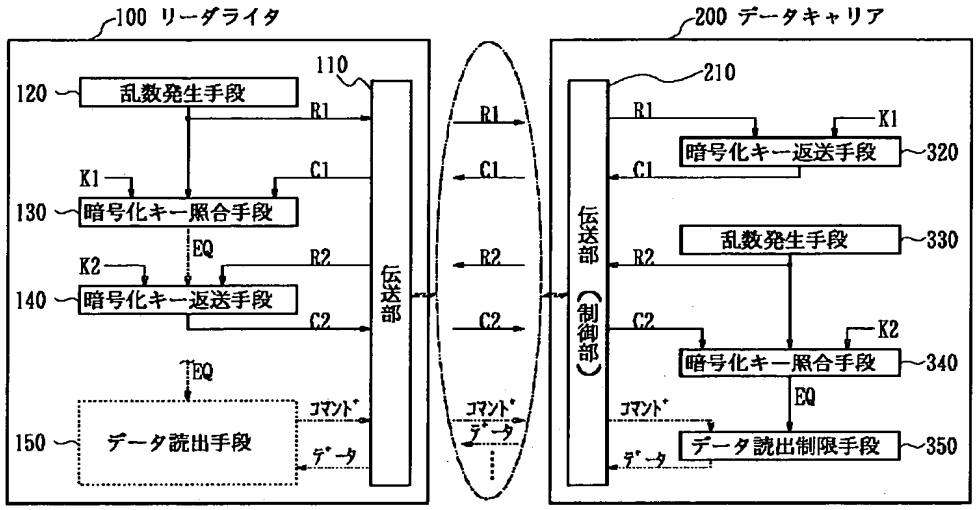
【図４】　従来のデータ秘匿装置である。

【符号の説明】

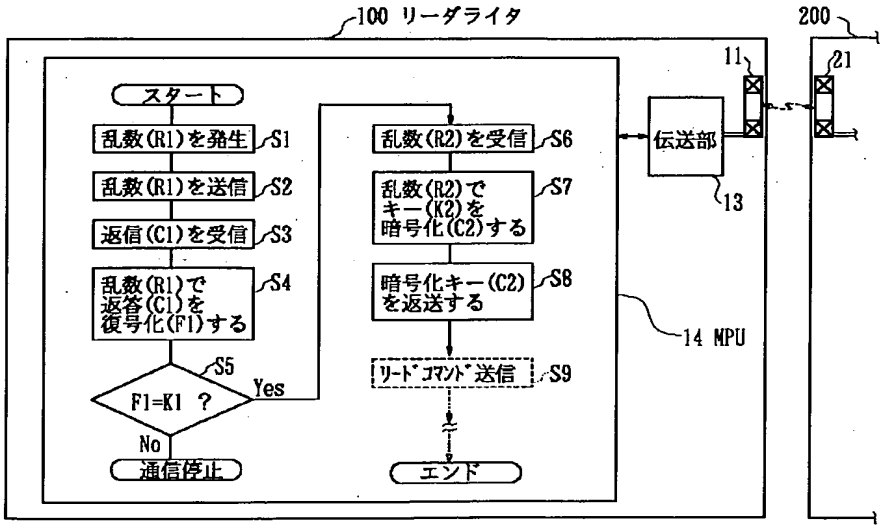
１０　リーダライタ（データ読取装置）
１１　コイル（アンテナ；電磁誘導結合子）
１３　伝送部
１４　マイクロプロセッサ（ＭＰＵ）
２０　データキャリア（携帯形データ記憶体）
２１　コイル（アンテナ；電磁誘導結合子）
２２　整流回路（電源回路）
２３　制御回路（制御部；伝送部）
２４　メモリ
３０　秘匿回路
３１　シフトレジスタ（第１秘匿解除データ保持部）
３２　シフトレジスタ（第２秘匿解除データ保持部）
３３　比較回路（照合手段）
３４　カウンタ
３５　順序回路（判定部；データ読出制限手段）
４１　ＡＮＤゲート（データ読出制限手段）
１００　リーダライタ（データ読取装置）
１１０　伝送部
１２０　（第１）乱数発生手段
１３０　（第１）暗号化キー照合手段
１４０　（第２）暗号化キー返送手段
１５０　データ読出手段
２００　データキャリア（携帯形データ記憶体）
２１０　伝送部
２３０　制御回路
３００　秘匿回路
３０１　シフトレジスタ（受信乱数Ｒ１保持部）
３０２　シフトレジスタ（読出キーＫ１保持部；秘匿解除データ保持部）
３０３　暗号化回路（暗号化キーＣ１返送手段）
３０４　乱数発生回路（乱数Ｒ２発生手段）
３０５　シフトレジスタ（発生乱数Ｒ１保持部）
３０６　暗号化回路（暗号化キーＣ２照合手段）
３２０　（第１）暗号化キー返送手段
３３０　（第２）乱数発生手段
３４０　（第２）暗号化キー照合手段
３５０　データ読出制限手段
ＣＳ　チップセレクト

ＳＫ　シフトクロック
ＤＩ　受信データ
ＤＯ　読出データ
ＥＱ　一致出力
ＣＮＴ　カウント値
＊ＫＩ、Ｋ２　キー（秘匿解除データ）
Ｒ１，Ｒ２　乱数（疑似乱数）
Ｃ１，Ｃ２　暗号化キー（乱数で暗号化された秘匿解除データ）
＊

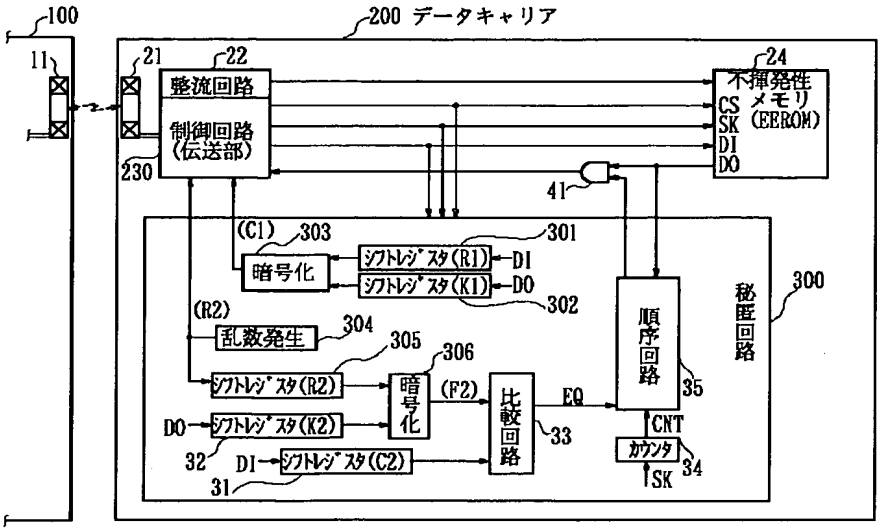
【図１】



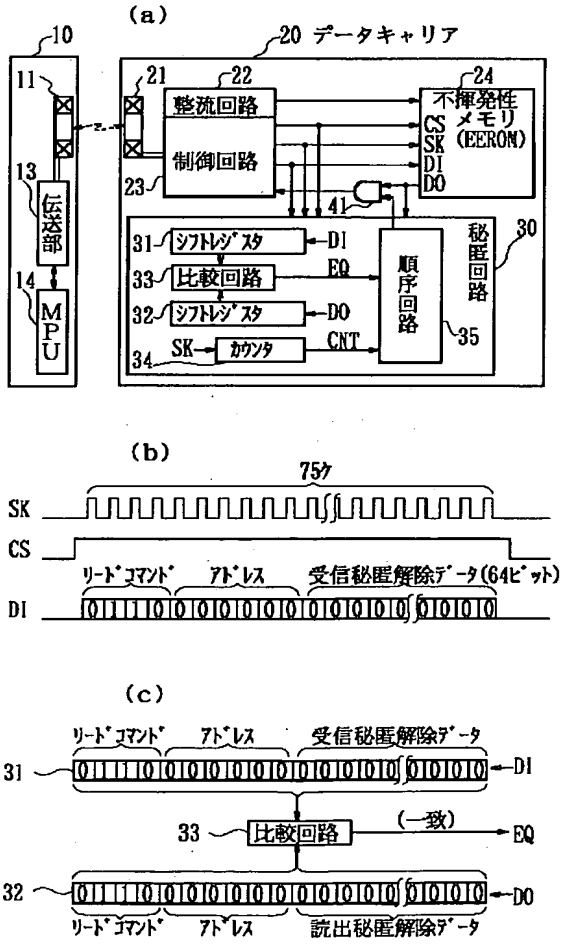

【図２】



【図３】


100
200 データキャリア
11
21
22
整流回路
制御回路
(伝送部)
230
24
不揮発性
メモリ
(EEROM)
CS
SK
DI
DO
41
(C1)
303
暗号化
シフトレジスタ(R1)
シフトレジスタ(K1)
301
302
(R2)
乱数発生
304
305
306
シフトレジスタ(R2)
暗号化
(F2)
比較回路
33
EQ
順序回路
35
秘匿回路
300
CNT
カウンタ
34
SK
DO
シフトレジスタ(K2)
32
DI
シフトレジスタ(C2)
31

【図４】


(a)
10
20 データキャリア
11
21
22
整流回路
制御回路
23
24
不揮発性
メモリ
(EEROM)
CS
SK
DI
DO
41
13
伝送部
14
MPU
31
シフトレジスタ
DI
33
比較回路
EQ
32
シフトレジスタ
DO
34
SK
カウンタ
CNT
順序回路
35
秘匿回路
30
(b)
75ク
SK
CS
リードコマンド
アドレス
受信秘匿解除データ(64ビット)
DI
(c)
リードコマンド
アドレス
受信秘匿解除データ
31
DI
33
比較回路
(一致)
EQ
32
DO
リードコマンド
アドレス
読出秘匿解除データ